KTH Computer Science
and Communication

Proof of Work

An evaluation of proof of work as a DOS prevention method

FREDRIK LILKAER, CHRISTOPHER TELJSTEDT

Bachelor's Thesis
Supervisor: Douglas Wikström

Chapter 1

Introduction

One of the most significant threats in server security are Denial of Service (DoS) attacks. It is essentially a targeted effort to prevent a service from functioning properly by draining the underlying computer resources. There are different levels of the attacks which either can be targeted to exploit vulnerabilities in the TCP/IP-protocol, in the operation system that the server runs on or more specific implementations of the service.

Recently, researchers have shown an increased interest in the Proof of Work (PoW) concept in order to prevent or mitigate the effects of a DoS attack on such a system. The idea is to require the clients to solve an instance of a predefined problem to gain access to the server's resources. The solving of the problem would decrease the rate that each client would be able to issue requests to the server. This reduces the total number of requests that reach the content server in any given timeframe to a level l. l could be tuned to a level lower than the server's inherent threshold of requests able to execute in said timeframe.

1.1 Purpose

The purpose of this study is to research ways to improve the classical Proof of Work in such a way that legitimate users are less affected by the Proof of Work than the participants of a DoS attack. Furthermore find a way to dynamically scale the required proof of work when dealing with different hardware.

Chapter 2

Background

The Denial of Service (abbr. DoS) is a class of cyber attacks directed to attack the availability of a web service. The typical DoS attack exploits the server by generating excessive memory and/or CPU utilisation of the server. Popular examples include SYN spoofing attacks which triggers the server to allocate input buffers for connections that never complete initiation as well as SSL attacks in which the server CPU is overloaded with expensive public-key decryption calculations.

One of the big challenges when facing DoS attacks is to distinguish between a legitimate user and an attacker. One approach is to block senders of erroneous packages, but when malicious users pose as legitimate this method certainly fails. The objective is to ensure the availability of the service to the legitimate users without infeasible delays.